Supervised secure entanglement sharing for faithful quantum teleportation via tripartite W states

Yue Li[*]

School of Computer Science and Technology and
Department of Electronics and Information Engineering,
Huazhong University of Science and Technology, Wuhan 430074, China

Yu Liu[†]

Department of Electronics and Information Engineering and
Institute of National Defense Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, China
(Dated: November 18, 2007)

We present a supervised secure entanglement sharing protocol via tripartite W states for faithful quantum teleportation. By guaranteeing a secure entanglement distribution in the charge of a third believed supervisor, quantum information of an unknown state of a 2-level particle can be faithfully teleported from the sender to the remote receiver via the Bell states distilled from the tripartite W states. We emphasize that reliable teleportation after our protocol between two communication parties depends on the agreement of the supervisor to cooperate via taking the W states as both the quantum channel and eavesdropping detector. The security against typical individual eavesdropping attacks is proved and its experimental feasibility is briefly illustrated.

Quantum teleportation (QT)[1] turns out to be incredibly successful in a wide variety of quantum information science, it achieves a different way for quantum state transmission, where arbitrary unknown quantum state collapses on the sender side and reborns on the receiver side via one way local operation and classical communication(LOCC) and previously shared pairs of maximal entanglement states.

To experimentally implement the QT, however, practical obstacles will be encountered. One is the *decoherence* and the *absorption* happen in the imperfect quantum channel[2], in which particles from entanglement pairs may get lost or entangled with the environment thus the entanglement decreases exponentially with the extension of the distribution distance. To address this, Zukowski *et al.* put forward the *entanglement swapping* to shorten the direct entanglement distribution[3], Bennett *et al.* introduced the *entanglement distillation* to refine the quality of entanglement effected by the decoherence after transmission[2]. Based on these two contributions, *quantum repeater*(QR), which was proposed by Briegel *et al.*, was constructed for long distance entanglement distribution in noisy and lossy quantum channel[4], the invention of QR makes long distance entanglement distribution possible and because the maximal entanglement pairs can be distilled from the imperfect entanglement ones, the assumption that entanglement distributions happen in a noise free environment becomes reasonable for QT-based quantum communication protocol design.

Another considerable obstacle is the security — *the potential eavesdropping.* Recently, various quantum communication protocols have been proposed based on the QT, most of which, however, are constructed under the popular hypothesis that the well known "third trustable party"(TTP) distributes the particles to the communication attendants without any interruption from the eavesdropper who may want to stole the sender's quantum information by recovering the qubits at her own hand, therefore, the protocol may not work well or even fail when the quantum channels are unauthenticated.

To be more general, the QT requires a secure enough quantum channel — for the direct quantum transmission to achieve the previous sharing of the entanglements — yet available channels are typically with evil quantum scientist who owns unlimited computing power. Through such considerations, we propose a supervised secure entanglement sharing protocol, the "Wuhan" protocol, for QT, in which a third supervisor Charlie is included to take in charge of the entanglement distribution and eavesdropping detection with classical communication and sequence of tripartite W states[5]. Under the help of this protocol, quantum information of an unknown state of a 2-level particle can be faithfully teleported.

The "Wuhan" protocol (see Fig. 1) enables faithful QT between Alice and Bob only when the TTP Charlie agrees to provide them the needed Bell states. The interesting scenario perfectly suits the bridge building rule in the Wuhan city. If a new Yangtse River bridge was going to be built between Wuchang(WC) and Hanyang(HY), two of the three member towns of the Wuhan city, should be approved by the governing town Hankou(HK) after which HK sends hardhats to WC and HY using HK-WC and HK-HY bridges respectively. Back from the tale, in this protocol we ask a believed supervisor Charlie to help the two parties Alice and Bob for distilling the "hardhat" — the Bell state

which is nondeterministically "hidden" in the following tripartite W state

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{abc}$$
$$= \sqrt{\frac{2}{3}}[\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{ab}]|0\rangle_c + \frac{1}{\sqrt{3}}|00\rangle_{ab}|1\rangle_c \qquad (1)$$
$$= \frac{1}{\sqrt{3}}(|++\rangle - |--\rangle)_{ab}|0\rangle_c + \frac{1}{2\sqrt{3}}(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle)_{ab}|1\rangle_c,$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Note that when measuring either of the three qubits, say particle c, Bell state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad (2)$$

made up of particles a and b can be obtained with a probability $P(|\psi^+\rangle) = \frac{2}{3}$, then the two communication parties cooperate with Charlie to execute two fundamental progresses, the *entanglement distribution*(ED) and *teleportation confirmation*(TC), in sequence. The ED helps to perform secure distribution of entanglement states to Alice and Bob; the TC, if Charlie permits, distills the "hidden" entanglement states for Alice and Bob by Charlie's local measurements. Here we give an explicit algorithm for "Wuhan" protocol, after which its security is discussed by examing several typical attacks.
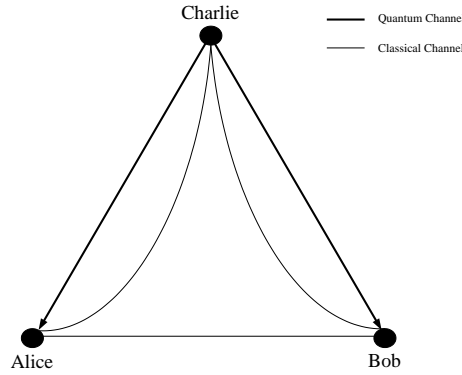

FIG. 1: The scenario of the "Wuhan" protocol.

(ED. 0) Protocol is initialized, $t = 0$. Charlie announces the switch to *transmission mode* and prepares three-qubit W states in EQ. 1, forming the sequence $w^N = (w_1, w_2, ..., w_i, ..., w_n)$, where $w_i = (a_i, b_i, c_i)$ are the three qubits of the ith W state. Here we assume the quantum state that Alice wants to teleport is

$$|\psi\rangle_m = a|0\rangle + b|1\rangle, \qquad (3)$$

where $|a|^2 + |b|^2 = 1$.

(ED. 1) $t = t + 1$. Charlie reserves qubit c_t from w_t as *home qubit*, sending the other two particles a_t and b_t to Alice and Bob respectively as the *travel qubits*. Repeat step (ED.1) until t reaches $n + 1$. As result, Charlie obtains a *home qubit* sequence $c^N = (c_1, c_2, ..., c_i, ..., c_n)$, and the two communicators are expected to obtain *travel sequences* $a^N = (a_1, a_2, ..., a_i, ..., a_n)$ and $b^N = (b_1, b_2, ..., b_i, ..., b_n)$ respectively.

(ED. 2) Charlie announces the switch to *detecting mode*, initializing $m = 1$. Starting from his particle c_m in c^N, Charlie performs a nondeterministic single qubit measurement using basis $B_z = \{(|0\rangle, |1\rangle)\}$, that is, the particle c_m owns a probability d to be measured and the whole W state collapses(also, $1 - d$ to be passed by without any operation). $m = m + 1$, repeat (ED. 2) until $m = n + 1$. Charlie takes down the locations of the particles measured, forming the location information sequence $k^V = (k_1, k_2, ..., k_i, ..., k_v)$ and related result sequence $Rc^V = (Rc_1, Rc_2, ..., Rc_i, ..., Rc_v)$ where k_i is the location of the ith measured particle in c^N satisfying $max(k^V) \leq n$, and Rc_i is the measurement result for the *home qubit* c_{k_i}. Also, Charlie selects v local measurement basises, each of which is in the B_x with probability p and B_x with $1 - p$, then he integrates the k^V and the basises into the sequence

$kb^V = ((k_1, b_1), (k_2, b_2), ..., (k_i, b_i), ..., (k_v, b_v))$ where $k_i \in k^V$ and $b_i \in \{B_x, B_z\}$, he then sends the kb^V to the classical channel, keeping the sequence Rc^V himself.

(ED. 3) Following the kb^V, Alice and Bob both perform local measurements on their own *travel qubit* sequences using the combined basis in kb^V, giving two measurement result sequences $Ra^V = (Ra_1, Ra_2, ..., Ra_i, ..., Ra_v)$ for Alice and $Rb^V = (Rb_1, Rb_2, ..., Rb_i, ..., Rb_v)$ for Bob. Unlike Charlie's keeping on Rc^V in Step (ED. 2), they send the two result sequences to the public classical channel.

(ED. 4) On receiving the two result sequences, Charlie performs the following checking algorithm for all elements of the two sequences:

> (Alg. 0) If $b_i = B_z$, let $\mathbb{C}[0]$ and $\mathbb{C}[1]$ be the two checking flags for Ra^V and Rb^V respectively;
> (Alg. 1) $\mathbb{C}[0] = 0$ if $Ra_i \oplus Rb_i = 0$ for all Rc_i s which are $|0\rangle$ in Rc^V, else $\mathbb{C}[0] = 1$;
> (Alg. 2) $\mathbb{C}[1] = 0$ if $Ra_i \oplus Rb_i = 1$ for all Rc_i s which are $|1\rangle$ in Rc_d^V, else $\mathbb{C}[1] = 1$;
> (Alg. 3) $(\mathbb{C}[0] \&\& \mathbb{C}[1]) = 0$: Eve is detected, Charlie announces the abortion of this distribution and goes to step (ED. 0); $(\mathbb{C}[0] \&\& \mathbb{C}[1]) = 1$: proceeds (TC. 0);
> (Alg. 4) Else, let $\mathbb{C}[2]$ be the checking flag;
> (Alg. 5) $\mathbb{C}[2] = 0$ if $Ra_i \neq Rb_i$ for all Rc_i s which are $|0\rangle$ in Rc^V, else $\mathbb{C}[2] = 1$;
> (Alg. 6) $\mathbb{C}[2] = 0$: Eve is detected, Charlie announces the abortion of this distribution and goes to step (ED. 0); $\mathbb{C}[2] = 1$: proceeds (TC. 0).

(TC. 0) Charlie ticks out all his measured *home qubits*, leaving the new *home qubit* sequence $c'^{N-V} = (c'_1, c'_2, ..., c'_i, ..., c'_{n-v})$ which are particles not selected in the *detecting mode*, if Charlie agrees with Alice and Bob's QT requirement, he performs local measurements on all the *home qubits* in c'^{N-V}, obtaining result sequence $Rc'^{N-V} = (Rc'_1, Rc'_2, ..., Rc'_i, ..., Rc'_{n-v})$. Note that after his measurements, the joint state of particles m, a and b may become one of the following states

$$
\begin{aligned}
|\phi_0\rangle &= |\psi\rangle_m \otimes {}_c\langle 0|W\rangle_{abc} \\
&= (a|0\rangle + b|1\rangle)_m \otimes |00\rangle_{ab}
\end{aligned}
\tag{4}
$$

$$
\begin{aligned}
|\phi_1\rangle &= |\psi\rangle_m \otimes {}_c\langle 1|W\rangle_{abc} \\
&= (a|0\rangle + b|1\rangle)_m \otimes \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{ab},
\end{aligned}
\tag{5}
$$

Charlie runs a selection to produce another location information sequence $k'^S = (k'_1, k'_2, ..., k'_i, ..., k'_s)$ satisfying $max(k'^S) \leq (n-v)$ and $Rc'_{k'_i}$ in Rc'^{N-V} is $|0\rangle$, then he publishes the sequence k'^V.

(TC. 1) According to k'^V, Alice and Bob locate and extract their own particles from a^N and b^N, taking particles $a_{k'_i}, b_{k'_i}$ as a whole, maximal entanglement pairs in Bell state $|\phi^+\rangle$ are successfully distilled and the required previous sharing is achieved, therefore further faithful QT between Alice and Bob can be pushed forward.

We now consider the security of the protocol and first take account of the intercept attack. Suppose the direction of the final QT are from Alice to Bob, it is sure that if Eve proposes only naive interceptions without appending fake particles, she may soon be detected when the three parties do the particle number comparison, therefore one considerable approach for Eve is the *intercept-resend attack* (IRA, see Fig. 2) which may include two different strategies, the *intercept-measure-resend attack* (IMRA) and the *intercept-store-resend attack* (ISRA), here we show the robustness of our protocol in case of these two IRA.

In the IMRA, Eve intercepts the particle which is going to the Bob side from Charlie and performs immediate single qubit measurement, then she appends fake particle which is identical with the measurement result to Bob which establishes fake quantum channel between Eve and Bob. To be more specific, because the initial state is $|W\rangle$, the evaesdropping may turns out to be in state $|0\rangle$ with probability $P(0) = \frac{2}{3}$, she then sends a fake particle in state $|0\rangle$ to Bob, thus joint state for Alice, Bob and Charlie's system becomes

$$
\begin{aligned}
|w_1\rangle &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{ac} \otimes |0\rangle_b \\
&= \frac{1}{\sqrt{2}}(|100\rangle + |001\rangle)_{abc};
\end{aligned}
\tag{6}
$$

or she may obtain state $|1\rangle$ with probability $P(|1\rangle) = \frac{1}{3}$, sending another particle in state $|1\rangle$ to Bob, leaving the
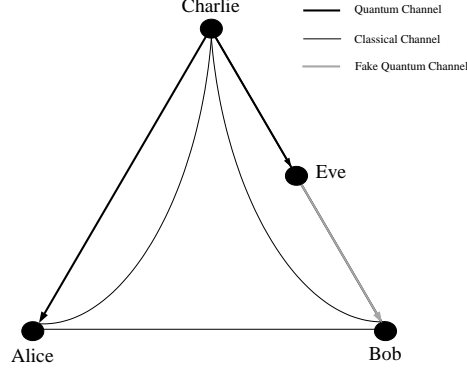
FIG. 2: Eavesdropping by the intercept-resend attack.

collapsed fake state

$$
\begin{aligned}
|w_2\rangle &= |00\rangle_{ac} \otimes |1\rangle_b \\
&= |010\rangle_{abc}.
\end{aligned}
\tag{7}
$$

In either case, we conclude that Eve can be detected with probability during the *detecting mode* of this protocol, however, we are going to ignore the calculations for these probabilities since the principals of the QT do not allow the collapsed but unentangled states $|w_1\rangle$ and $|w_2\rangle$ being the appropriate sources between Eve and Alice to recover Alice's quantum states, in other words, the IMRA can not bring Eve any quantum information.

Coming to the other IRA strategy, the ISRA, where Eve protects the intercepted particle by just storing without measurement to wait for a later impersonating teleportation. In order to hide her existence, Eve then sends a fake qubit from herself to Bob, different from the IMRA, Eve does not know the exact state of the particle, thus she can only send a particle in state $|\phi\rangle_{b(e)} = (x|0\rangle + y|1\rangle)_{b(e)}$ in which x, y are random coefficients satisfying $x^2 + y^2 = 1$, then the joint state of the quad-party system turns to

$$
\begin{aligned}
|\Upsilon\rangle &= |\phi\rangle_b \otimes |W\rangle_{aec} \\
&= (x|0\rangle + y|1\rangle)_b \otimes \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{aec} \\
&= \frac{1}{\sqrt{3}}(x|1000\rangle + y|0101\rangle)_{aecb} \\
&\quad + \frac{1}{\sqrt{3}}(x|0100\rangle + y|1001\rangle)_{aecb} \\
&\quad + \frac{1}{\sqrt{3}}(x|0010\rangle + y|0011\rangle)_{aecb}
\end{aligned}
\tag{8}
$$

For convenience, we ignore the intercepted particle e, and write the Eq. (8) into

$$
\begin{aligned}
|\Upsilon'\rangle &= \frac{1}{\sqrt{3}}(x|100\rangle + y|010\rangle)_{abc} \\
&\quad + \frac{1}{\sqrt{3}}(x|000\rangle + y|110\rangle)_{abc} \\
&\quad + \frac{1}{\sqrt{3}}(x|001\rangle + y|011\rangle)_{abc},
\end{aligned}
\tag{9}
$$

according to the checking algorithm in (ED. 4):

Case 1. If Charlie's measurement obtains state $|1\rangle$, combining the basis B_z with probability p, Eve may be detected due to the introduced state $|Rej_1\rangle = |011\rangle_{abc}$ with probability

$$
P(d_1) = \frac{1}{3} \cdot p \cdot d \cdot y^2 = \frac{pdy^2}{3};
\tag{10}
$$

Case 2. If Charlie obtains state $|0\rangle$ combining B_z, Eve may be detected by the state $|Rej_2\rangle = x|000\rangle + y|110\rangle$ with the probability

$$P(d_2) = \frac{1}{3} \cdot p \cdot d = \frac{pd}{3};$$ (11)

Case 3. If Charlie combines the basis B_x, the eavesdropping attack succeeds no matter what Charlie's measurement results.

Therefore, the probability of a successful ISRA eavesdropping for one particle is

$$
\begin{aligned}
S(y, p, d, 1) &= 1 - P(d_1) - P(d_2) \\
&= 1 - \frac{pd}{3} - \frac{pdy^2}{3} \\
&= 1 - \frac{pd(1 + y^2)}{3},
\end{aligned}
$$ (12)

and the rate for whole sequence w^N is

$$
\begin{aligned}
S(y, p, d, n) &= S(y, p, d, 1)^n \\
&= [1 - \frac{pd(1 + y^2)}{3}]^n.
\end{aligned}
$$ (13)

For $0 \leq y, p, d \leq 1$, $S(y, p, d, n)$ decreases exponentially but is always nonzero. In the limit $n \to \infty$, we have $S(y, p, d, n) \to 0$, thus the protocol is *quasi-secure*. Here we give the curves for $S(y, p, d, n)$ in Fig. 3 as examples for cases of different y, p, d selections.
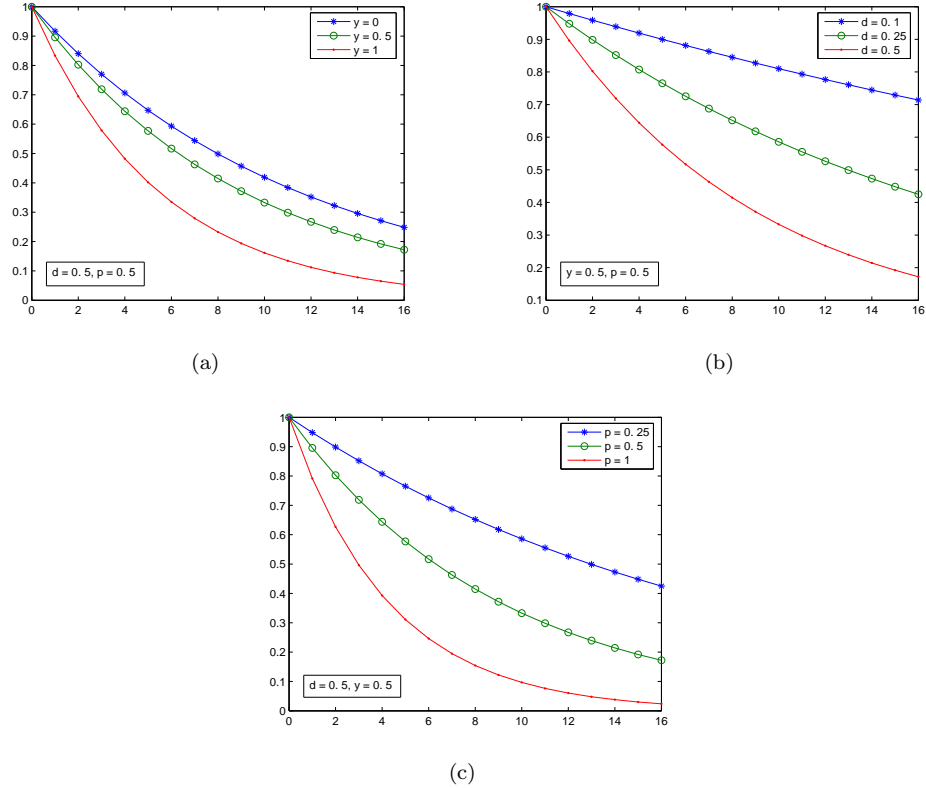

(a)

(b)

(c)

FIG. 3: Successful eavesdropping rates, plotted for (a) specified probability d and p with different state coefficients y; (b) specified y and p with different d; (c) specified d and y with different p

Another typical attack different from the IRA is the *entangle-measure attack*(EMA, see Fig. 4), i.e. Eve may uses her own *ancillar qubit* which is in state $|0\rangle$ to entangle with the *travel qubit* b being sent to Bob by utilizing a CNOT

gate U_{be} (let Bob's particle be the *controller* and Eve's be the *target*)[6], then the joint state of the four particles becomes

$$U_{be}|W_{abc}0_e\rangle = \frac{1}{\sqrt{3}}(|1000\rangle + |0101\rangle + |0010\rangle)_{abce}, \tag{14}$$

since the EMA never modifies the original state of the three-qubit W state, this kind of attack can not be sensed during the protocol, however, Eve can still be found during the final QT, the reason is that after Eve's CNOT operation, the extracted Bell state used for QT actually becomes $|\phi'\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{abe}$, with the state $|\psi\rangle_m$, we have the joint state

$$
\begin{aligned}
|\psi\rangle_m|\phi'\rangle_{abe} =& (a|0\rangle + b|1\rangle)_m \otimes \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{abe} \\
=& \frac{1}{\sqrt{2}}(a|0100\rangle + a|0011\rangle + b|1100\rangle + b|1011\rangle)_{mabe} \\
=& \frac{1}{2}|\psi^+\rangle_{ma}|\varepsilon^+\rangle_{be} \\
& + \frac{1}{2}|\psi^-\rangle_{ma}|\varepsilon^-\rangle_{be} \\
& + \frac{1}{2}|\phi^+\rangle_{ma}|\xi^+\rangle_{be} \\
& + \frac{1}{2}|\phi^-\rangle_{ma}|\xi^-\rangle_{be},
\end{aligned}
\tag{15}
$$

where $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\varepsilon^\pm\rangle = (a|00\rangle \pm b|11\rangle)$ and $|\xi^\pm\rangle = (a|11\rangle \pm b|00\rangle)$, Eve may recover the state that Alice teleports on the first particle of her *ancillar qubit* sequence, however if Eve continues to perform measurement for specifying the coefficients a and b, the entanglement state made up from particles b and e collapses, therefore Bob's measurement on his particle thus only gives deterministic result, which implies Eve's existence.
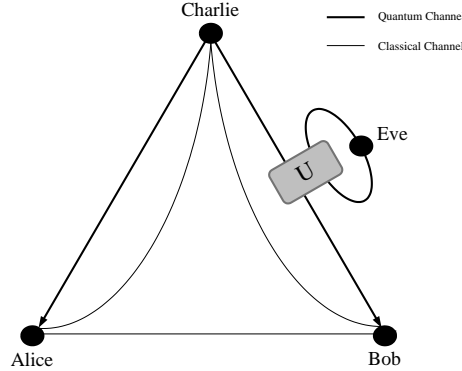

FIG. 4: The entangle-measure attack.

The "Wuhan" protocol is experimentally feasible. The tripartite W states can be produced by the parametric down-conversion method[7]; the storage of photons is necessary only for a duration corresponding to the distance of Charlie's distributions and the quantity of qubits that Alice wants to teleport and the entanglement sharing efficiency depends on Charlie's checking parameters d and p; the local measurements and the QT have been already experimentally implemented. Altogether, the realization of the "Wuhan" protocol should be reachable using current quantum information technology.

---

* Electronic address: liyue@smail.hust.edu.cn

† Electronic address: liuyu@hust.edu.cn

[1] C. H. Bennett, G. Brassard, C. Crpeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennet, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[3] M. Zukowski, A. Zeilinger, M. A. Home, A. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[4] H. J. Briegel, W. Dür, J. I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5933 (1998).
[5] W. Dür, G. Vidal, J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[6] M. A. Nielsen, I. L. Chuang, *Quantum Information and Computation* (Cambridge University Press, Cambridge, 2000).
[7] D. Bouwmeester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information* (Springer, New York, 2000).